Prepared Testimony and Statement for the Record of
Marc D. Gordon
Executive Vice President and Chief Information Officer
American Express

Before the
United States Senate
Committee on Homeland Security and Government Affairs

Hearing on "Protecting America from Cyber Attacks: The Importance of Information Sharing"

Wednesday, January 28, 2015

Chairman Johnson, Ranking Member Carper, members of the Committee, my name is Marc Gordon and I am Executive Vice President and Chief Information Officer at American Express. In this role, I oversee the technology organization that is helping to drive the digital transformation of the company through innovative technology solutions that are powering revolutionary products and experiences across the commerce cycle. I also oversee the delivery and operations of technology capabilities and services globally, as well as information security for the Company.

I appreciate the opportunity to testify about the serious threats we face today and my views on information sharing programs. Based on my roles in multiple global fortune 100 firms and the experiences I have had in information sharing within and across sectors, I would strongly urge the Committee to swiftly move forward with information sharing legislation. While effective information security requires a web of inter-related controls, I believe effective information sharing may be the single highest impact/lowest cost/fastest to implement capability we have at hand as a nation to accelerate our overall defense from the many and varied and increasing threats around us.

Threat Landscape

The threat environment today is increasingly complex, increasingly challenging and constantly changing. While defending our networks, protecting sensitive information and making our services available to our customers as part of an increasingly digital economy, we operate in an environment where:

- In 2014, we received over 5000 FS-ISAC cybersecurity alerts providing information of a variety of threats, attacks and other information supplied by members for members (an example of information sharing that goes on today),

and have received approximately 100,000 technical indicators (describing malicious IP addresses, websites, malicious code components or some other aspect of a cyber threat to help maintain our defenses) from a variety of intelligence sources.

- Distributed denial of service (DDoS) attacks, where attackers send so much internet traffic to a company's website as to render the site unavailable to legitimate consumers, have more than tripled in strength in the last 18 months, challenging even the best defended companies to maintain availability of vital web services to their customers. (source – Prolexic Q3 2014 State of the Internet Security report)
- During the last year, there were nearly 60 million records compromised in reported security breaches affecting businesses, including financial institutions and retailers. (source – Privacy Rights Clearinghouse)
- The increasing use of 'ransomware' to encrypt a victim's entire computer and extort them for money to regain access to their files is especially pernicious and threatens consumers and corporations alike. One estimate indicated that over $27 million in ransom payments were made in just the first two months since a common ransomware known as *Cryptolocker* was first discovered in late 2013. (source – FBI.gov, June 2014 Issue 62)

While cyber crime is growing meaningfully across industries, and that is a clear concern, we are also increasingly concerned about the convergence of players, capabilities and intentions: as reported in the press, nation state players with destructive intention and capability that have targeted various industries.

Information Sharing Legislation

In response to the threats above, the financial services industry has invested billions of dollars to protect our networks from cyber attacks. These investments are expected to continue and in most cases accelerate.

In addition to the investments being made across industries, there are steps we can take to make the total ecosystem more secure, beginning with the right private/public partnerships that can help companies better protect themselves. This requires Congressional guidance. Meaningful legislation would greatly expand the quality and volume of cyber information sharing; raise the level of security overall; and reduce the variability of security within and across industries both for critical infrastructure and non-critical infrastructure organizations.

Today, members of the financial services industry have a mechanism for sharing threat data with one another. Through our FS-ISAC, or Financial Services Information Sharing and Analysis Center, we securely share cyber threat information including threat signatures used in certain attacks. The FS-ISAC also allows the industry to exchange threat data regarding tools, techniques and procedures that help alert the broader financial services community of impending threats. Venues like the National Cyber Forensics Training Alliance, or NCFTA, provide an opportunity to collaborate closely with law enforcement to combat the problem of cyber crime and help protect customers, banks and retailers alike.

Despite this, more information could be shared within and between industries. In addition, industry should be able to more freely send and receive threat data from the government. Unfortunately, there are existing legal barriers to us doing so, including the

threat of lawsuits, and that is where Congressional guidance is desperately needed. Legislation that provides targeted protections from liability and disclosure – both for business-to-government sharing but also for business-to-business sharing – is sorely needed. By affording targeted protections from liability and disclosure, entities across sectors will be more willing to share key threat data without fear of unnecessary and wasteful litigation or public disclosures that could further compromise their systems. This could allow, for instance, a member of the Financial Services sector to provide threat data to the retail sector, which could potentially prevent the next major breach, or protect from the potential loss or destruction of customer information, or the theft of intellectual property. Without these targeted protections we lose a real opportunity to improve the security of the overall ecosystem.

Further, statutory protection from Freedom of Information Act (FOIA) requests related to cyber threat information shared with the government would help improve the information sharing frameworks that exist today. The lack of a FOIA exemption undercuts the very intent of more effective voluntary information sharing by allowing public access to the sensitive threat information organizations voluntarily provide. Once the information is public, it could be used by bad actors searching for system weaknesses or other information that may help them accomplish their cyber objectives. As a result, an organization's willingness to share such information diminishes greatly.

Significant progress was made in the last Congress towards enactment of meaningful information sharing legislation. Multiple industries, law enforcement, and cybersecurity experts worked with committees in both the House and Senate to develop bipartisan legislation. Though there were modest differences in the approaches taken by

the House and Senate, these bills can serve as a template for the new Congress. There are a few notable items we would emphasize in terms of attributes of information sharing that we believe are important:

- real time sharing: threats unfold in minutes and hours and cascade company to company and sector to sector rapidly; sharing needs to be real time to be most effective
- liability and disclosure protection needs to include not just the sharing itself, but 'good faith' action taken (within the company's network and systems) based on the information shared; otherwise sharing itself may not result in the necessary action being taken
- companies should be protected from sharing among themselves, not just with the government or government sanctioned entities, to ensure every opportunity to protect systems is available
- sharing needs to be bi-directional; the ecosystem is much stronger when indicators only known/knowable by the government are shared back to the private sector; we would encourage the legislation to include active and clear requirements for this to occur
- effective sharing will require a designated 'hub' within the government for bi-directional sharing but should also not prevent other public/private sharing from occurring

Finally, we recognize that there are important privacy questions that must be answered as part of information sharing legislation; we are committed to protecting the

privacy of our customers' information; and believe that concerns around privacy protection can be effectively addressed.

Conclusion

I want to thank you again for asking me to be here today. We truly appreciate the opportunity to share our views on this important issue, and we look forward to working with this Committee, and other members of the Senate and the House going forward. This concludes my prepared remarks. I would be happy to answer any questions that you may have.